(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 935 182 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
11.08.1999 Bulletin 1999/32

(51) Int. Cl.[6]: **G06F 1/00**

(21) Application number: **98300144.7**

(22) Date of filing: **09.01.1998**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant:
Hewlett-Packard Company
Palo Alto, California 94304 (US)

(72) Inventors:
- **Chan, David**
  Henleaze, Bristol (GB)
- **Gupta, Dipankar**
  Bristol (GB)
- **Van Wilder, Bruno**
  Bristol (GB)

(74) Representative:
Lawman, Matthew John Mitchell et al
Hewlett-Packard Limited,
IP Section,
Building 2,
Filton Road
Stoke Gifford, Bristol BS12 6QZ (GB)

(54) Secure printing

(57) In a distributed computing environment, a user is able to send a document to a secure printer 140 in such a way that only the intended recipient can print the document. When the user specifies that the document is to be printed securely, a special print job is created in which the document is encrypted under the recipient's public key. Then, when a print server 130 receives the print job, it is incapable of printing it, as it is encrypted, and the job is held. When the recipient's smart card 145 is inserted into a smart card reader of the secure printer 140, the recipient's identity from the smart card is used to search for and retrieve documents from the print server 130 for the recipient, and private key information on the smart card 145 is used to enable decryption and printing of the document by the printer.

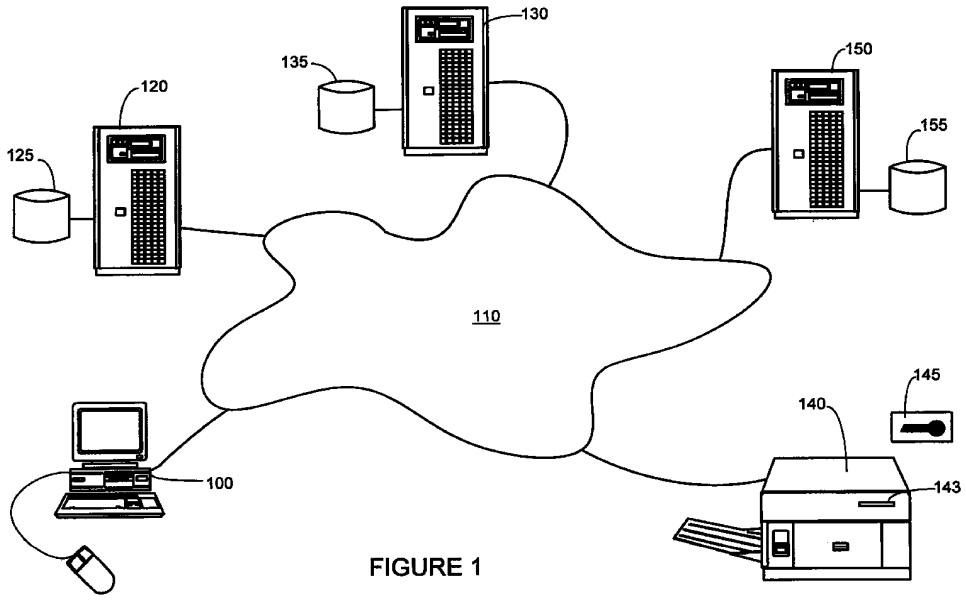

FIGURE 1

EP 0 935 182 A1

Description

Technical Field

[0001] The present invention relates to hardcopy production of documents and particularly, but not exclusively, to document printing.

Background Art

[0002] It is well known to generate or design a document using a computer-based text editing or graphics package, for example Microsoft Word or Microsoft Excel respectively. Once generated, a document is typically formatted by the package into a data file that comprises, for example, PCL or PostScript data, which is interpretable by a hardcopy device such as a printer. The document data file can be sent directly by the package to a printer to be printed, or can be stored for printing at a later time.

[0003] This principle typically applies to all types of printer, for example laser printers, ink jet printers, impact printers and thermal printers, and in general to other hardcopy devices such as plotters or facsimile machines.

[0004] For the sake of convenience of description herein, the term "document" will hereafter be used as a convenient term to denote a document in any state, including when viewed on a computer display, when formatted as a hardcopy apparatus-readable data file ready for rendering, and when in hardcopy form. The state the document at any point in the description depends on the context. Also, the term "document" will be used to describe a textual, graphical, or mixed representations.

[0005] The advent of distributed computer systems has made it possible for a single 'network' printer to be used by multiple users. Typically, network printers are attached to computing platforms operating as print servers within distributed systems. Alternatively, some printers, given appropriate interfaces, can be arranged to connect directly to the network of a distributed system.

[0006] Network printers, whether connected directly, or via a print server, to a network, can provide a substantial cost advantage, since each user need not have his own printer connected to, or located near to, his own computer system.

[0007] The ability to access network printers, and other devices, from a local computer, is readily supported by operating systems such as Unix, or Microsoft's Windows NT, which are designed to be configured to manage distributed operations such as remote printing or data management.

[0008] One problem with printing documents on remote network printers is that any person near to the printer could remove or read printed documents containing sensitive information, which do not belong to them, before the correct recipients are able to retrieve the documents. One way around this is for users who need to print sensitive documents to arrange for a trusted person to stand by the printer while the document is printing and collect the document as soon as it has printed. This is, of course, inconvenient.

[0009] Another way to increase security is to print sensitive documents only on a local printer. The latter case, however, undermines any cost advantages gained in having a centrally located, network printer, especially if many users need to print sensitive documents.

[0010] Another problem associated with remote printing of sensitive documents is that a malicious party could intercept or monitor the transfer of data between the local computer and network printer. For example, anyone with access to a print spooler or print server receiving the document for printing could access the document. This would be highly undesirable and, again, could be overcome by using a local printer attached directly to the originating computer instead.

Disclosure of the Invention

[0011] Aspects of the present invention aim to increase the security of remote printing.

[0012] In accordance with a first aspect, the present invention provides hardcopy apparatus comprising interface means for receiving from a document store an encrypted document, processing means configured for decrypting the encrypted document and rendering means for producing a hard copy of a decrypted document.

[0013] This aspect of the invention provides a secure mechanism in which a document can be encrypted prior to it being sent for rendering by the hardcopy apparatus. The hardcopy apparatus, such as a printer, is configured to receive and decrypt encrypted documents prior to producing a hard copy of the document.

[0014] Thus, even if a document were intercepted during transfer between a computer and network printer, say, it would be a non-trivial task for the intercepting party to decrypt the document.

[0015] In a preferred embodiment of the invention, the hardcopy apparatus further comprises input/output means for communicating with a removable processing means.

[0016] Preferably, the input/output means is a smart card reader and the removable processing means is a smart card received by the smart card reader.

[0017] The processing means may then be configured for receiving information from the smart card reader, when a smart card is received thereby, and using the information to retrieve and decrypt an encrypted document. It would be possible to supply the information using, for example, a keypad, or even a swipe card reader, but a smart card is perceived by the applicants to be far more convenient.

[0018] In a preferred embodiment, the processing means is configured for receiving from the smart card

an identity, sending a first message via the interface means to the document source, the message including at least an indication of the identity, and receiving from the document source via the interface means, in response to the first message, a return message including at least an encrypted session key for an encrypted document stored by the document source and having a matching identity.

[0019] Thus, the identity on the smart card is passed to the document source in order for the document source to search for and return an encrypted session key for any documents that have a matching identity. At this stage, the document source may also return the encrypted document. However, this would depend on the amount of storage available to the hardcopy device for temporarily storing documents.

[0020] The hardcopy apparatus is then, preferably, configured for sending the encrypted session key to the smart card reader, for the smart card to extract the session key, and receiving back the session key. The processing means may then be configured for using the session key to decrypt the encrypted document.

[0021] This approach has the advantage that the private key used to decrypt the session key need not leave the smart card. The implication of this is that the overall mechanism relies on a secret that never becomes known to the printer or any other part of the distributed system.

[0022] Typically, the document store takes the form of a special print server which is configured to receive encrypted documents for printing and storing the documents until a request message for a document is received from, for example, hardcopy apparatus configured according to the present invention. The form of the document store will be described in more detail below.

[0023] In this way, the actual hardcopy production can be initiated by a user inserting a smart card into the hardcopy apparatus's smart card reader at any time alter the encrypted document has been submitted to the document store.

[0024] This has the advantage that once a document has been submitted for rendering, it is held by the document store until a remote party inserts a smart card into a remote hardcopy apparatus. Accordingly, the hardcopy of the document is only produced when it is convenient for the recipient, who may or may not be the same person as the sender, to retrieve the document in person.

[0025] Preferably, the information received from the smart card includes an identity, for example the identity of the owner of the smart card, and the hardcopy apparatus is configured to send a message including the identity to the document store. In response, the document store can determine whether it has a stored document with a matching identity, and forward the document to the hardcopy apparatus. Typically, in this case, documents will be submitted with associated identity information to the document store for rendering.

[0026] In the preferred embodiment to be described, a user is able to send a document to a secure printer in such a way that only the intended recipient can print the document. When the user specifies that the document is to be printed securely, a special print job is created in which the document is encrypted under the recipient's public key. Then, when the document store receives the print job, it is incapable of printing it, as it is encrypted, and the job is held. When the recipient's smart card is inserted into the secure printer, the recipient's identity from the smart card is used to search for and retrieve documents for the recipient, and private key information on the smart card is used to enable decryption and printing of the document by the printer.

[0027] In accordance with a second aspect, the present invention provides a method of controlling hardcopy apparatus to render an encrypted document, comprising the steps of retrieving from a document source an encrypted document, decrypting the encrypted document, and rendering the document to produce a hardcopy thereof.

[0028] In accordance with a third aspect, the present invention provides a computer system arranged for secure rendering of documents, the system comprising secure printing means for encrypting a document for an intended recipient and forwarding to a document store means the encrypted document with identity information of the intended recipient, document store means for receiving encrypted documents and respective identity information and storing said encrypted documents and respective information, and for receiving requests from hardcopy apparatus for documents having a specific identity and sending respective documents to the respective requesting hardcopy apparatus, and hardcopy apparatus arranged for requesting of the document store means transfer of encrypted documents having a specific identity, decrypting received documents and rendering in hardcopy form decrypted documents.

[0029] In accordance with a fourth aspect, the present invention provides a document server, comprising document processing means arranged for receiving encrypted documents, storing encrypted documents, receiving requests for specific documents, searching the stored documents for the specific documents, and returning found documents to the requesting party.

Brief Description of the Drawings

[0030] An embodiment of the present invention will now be described, by way of example only, with reference to the accompanying drawing, of which:

Figure 1 is a diagram which illustrates a distributed computing environment which supports secure printing in accordance with an embodiment of the present invention;

Figure 2 is a block diagram of an architecture for a

printer according to the present embodiment;

Figure 3 is a flow diagram which illustrates the steps involved in a user submitting a document for secure printing; and

Figure 4 is a flow diagram that illustrates the steps involved in a secure printer retrieving and printing a print job.

Best Mode For Carrying Out the Invention, & Industrial Applicability

[0031] The following description refers specifically to a printer as the hardcopy device. However, it is emphasised that the same principles apply to other hardcopy apparatus such as facsimile machines.

[0032] In Figure 1, a local computer 100, for example an Intel Pentium based computer operating under Windows NT 4.0, includes the standard components of a keyboard, a display and a mouse (none of which are shown). The local computer 100 is attached to a network 110, for example a network supporting the TCP/IP protocol. The local computer 100 provides a secure printer process, which is a software routine that can be initiated by a user when secure printing is required. The process, and all other processes in this embodiment, can be written in any general purpose programming language, such as Visual C++.

[0033] Also connected to the network 110 are a directory server 120, a document store 130, a secure printer 140 and billing engine 150.

[0034] The directory server 120 is a process running on a computer, which has access to a database 125 of user-specific information, known as user-profiles. The directory server 120 is arranged to receive from requesting processes requests for specific information for particular users, and returns the specific information to the requesting process, whenever possible. The computer running the directory server 120 could be a Unix or Windows NT platform connected to the network 100 via an appropriate interface. The directory server 120 in the present embodiment is a simple database, which receives enquiries and returns relevant data, but it could be based on purpose built directory services such as Novell's NDS or Microsoft's Active Directory. In accordance with the present embodiment, the directory server 120 is configured to receive a request including a user identity and return at least a public encryption key associated with the identified user. Communications with the directory server 120 may be with a network protocol such as the Lightweight Directory Access Protocol (LDAP).

[0035] The document store 130 is process running on a computer which receives and stores encrypted document files and associated user identities. The document store 130 also receives requests to forward to specified locations encrypted document files having a specified identity. Again, the computer running the directory server 120 could be a Unix or Windows NT platform connected to the network 100 via an appropriate interface.

[0036] In practice, the document store 130 can be a modified print spooler or print server process, which has access to a large amount of data storage, for example provided by a disk drive 135. The spooler or server is modified in the respect that it is arranged to recognise encrypted documents and, rather than forwarding them to a specific printer, hold or store the encrypted documents. The spooler or server is also modified to receive requests from printers for specific encrypted documents, search for the specified encrypted documents and transfer the encrypted documents to the requesting printer.

[0037] It should be noted that the document store 130 in the present embodiment is an untrusted part of the distributed system, in that the document store 130 is configured to return documents to any requesting printer, or other device using an appropriate protocol. The present embodiment relies on the security of the strong encryption applied to the document to protect the information in the document.

[0038] In other embodiments, where security is even more important, it is envisaged that the document store 130 would further incorporate authentication functionality, which would allow the document store to authenticate either the requesting printer or smart card user. Authentication systems using, for example, digital signatures are well known and will not be considered herein in any more detail.

[0039] The architecture of the printer 140 according to the present embodiment is illustrated in more detail in Figure 2. Figure 2 illustrates a central processing unit (CPU) 200 that controls a print engine 210, which is a standard part of any printer that enacts printing, and the details thereof are beyond the scope of the present description. A read only memory (ROM) 220 is connected to the CPU 200 by an appropriate system bus 205. The ROM 220 contains the instructions that form the control program for the printer. Also connected to the system bus 205 is non-volatile memory (NV-RAM) 230 and main memory (DRAM) 240. The NV-RAM 230 can be E2PROM or Flash RAM for receiving and storing services downloaded into the printer. The DRAM 240, is used by the printer as buffer memory, for receiving jobs to be printed, and is also used by the CPU 200 in the present embodiment as workspace for decryption and session key storage. All the features of the printer 140 described so far are standard on many generally available printers. The diagram also illustrates the standard printer features of a network interface 250, various sensors 260, for example 'paper out', and a front panel display and keypad 270, all connected to the CPU via the system bus 205. Finally, a smart card reader 280 is provided, also connected to the system bus 205, although it could alternatively be connected via the printer's RS232 port, where one is available. Thus, the only significant, non-standard hardware feature of the printer is

the smart card reader 280. The other differences depend on software or firmware processing.

[0040] Smart card readers are generally available and conform to accepted standards. The smart card reader used in the present embodiment supports the ISO 7816 standard (levels 1 to 4), and some extra functionality not covered by the ISO standard, which is described herein. Corresponding smart cards are also readily available, and are programmable to operate as described herein.

[0041] In practice, the smart card reader can be incorporated into the casing of a standard printer. Thus, in this case, the only significant, noticeable difference about the printer is a slot 143 in the casing into which a smart card 145 can be inserted and retrieved.

[0042] Printers which generally have the features illustrated in Figure 2 are a Hewlett-Packard LaserJet 5 or a Hewlett-Packard LaserJet 4000. In either printer, the printer's conventional control program can be modified as described herein, by either replacing the printer's firmware, in ROM 220, or by creating a 'service', which can be downloaded into the printer's flash memory, NVRAM 230, from the network.

[0043] Details on how to modify control programs in Hewlett-Packard and others' printers are beyond the scope of the present description, but are readily available from Hewlett-Packard Company or from the respective other printer manufacturers.

[0044] The billing system 150 is a process running on a computer which electronically bills users of the secure printing system. There are three main areas where users could be billed, which are for: submission of an encrypted document to the document store 130, storage by the document store 130 of a document for a specified time; and transmission and successful printing of the document. Other acts, such as using the directory server 120, could potentially also be billed. The sender or the recipient, or both, could be billed for any or each of these acts. For example, the sender could be billed for the submission, and the recipient could be billed for the storage and printing of the document. Of course, the sender and the recipient might be the same person, or different people from the same organisation, in which case a single person or organisation respectively would be billed for everything. Further, the owner of the document store and the owner of the printer might be different independent service providers. For example, in the case where the printer is in a public place, and is for use by the public, then the printer's owner would want financial reward for providing the service. Therefore, it would be necessary for a printer to identify itself in enough detail that the billing system 150 could allocate billed funds to the printer's owner.

[0045] For every act, it is necessary to identify the party to be billed and the party to be paid. Electronic identification and authentication for the purposes of electronic billing are well known in the field of electronic commerce, and will not therefore be discussed in any more detail herein.

[0046] The operation of the local computer 100 in submitting a secure print job will now be described with reference to the flow diagram in Figure 3.

[0047] In step 300 of Figure 3, the local computer's operator (not shown), in other words the document's sender, has a document, for example a word-processed document, to be submitted for printing. The sender initiates the secure printing process for the secure printing of the document, in step 305. The secure printing process, in step 310, generates a graphical user interface, which requires the sender to enter the document details and the identity of the intended recipient. Of course, the intended recipient might be the sender himself. The sender enters the required details in step 315. Having received a valid input from the sender, the process, in step 320, continues by transmitting a request including the details input by the sender to the directory server 120. In response, the directory server 120 returns to the secure printing process the public key for the intended recipient, in step 325.

[0048] Next, in step 330, the secure printer process formats the document into a page description language, such as PostScript or PCL, which is interpretable by a printer. Obviously, the language will depend on the type of printer or other hardcopy apparatus to be used. The secure printer process then, in step 335, applies bulk encryption to the formatted document while retaining its integrity. This can be achieved using a message digest function such as the Secure Hash Algorithm (SHA-1) and a symmetric block or stream cipher, for instance, Data Encryption Standard (DES). The cipher uses a random number generated by the secure printer process to enact the encryption. The random number constitutes a session key. This step is a symmetric encryption step, which relies on a recipient having access to the session key to decrypt the document.

[0049] Alternative message digest algorithms, such as MD5, symmetric ciphers such as CAST or IDEA, and asymmetric algorithms such as the Elliptic Curve ElGamal encryption scheme can be used instead of the algorithms specified earlier.

[0050] In step 340, the secure printer process then applies an asymmetric encryption algorithm, such as RSA, to the session key, using the intended recipient's retrieved public key. Thus, alter this step, only someone who has knowledge of the private key associated with the public key can decrypt the session key and hence then decrypt the document.

[0051] In step 345, the secure printing process forwards across the network 110, to the document store 130, a message comprising the encrypted document, an 'envelope' for the document (which contains the encrypted session key), and the respective identity of the intended recipient.

[0052] Finally, in step 350, the document store 130 receives the message and stores it appropriately to hard disk 135.

[0053] The process of securely printing a document

retrieved from the document store 130 will now be described with reference to the flow diagram in Figure 4.

[0054] In step 400 of Figure 4, the intended recipient of the document, which has been stored by the document store 130 as described already, inserts his smart card into the smart card reader 280 of the secure printer 140. The smart card includes the recipient's identity and the recipient's private key. Although not illustrated in the flow diagram, it would be typical at this stage for the printer 140 to request entry by the recipient of a personal identification number, to verify that the recipient is the genuine owner of the smart card, and not someone who has found, or even stolen, it.

[0055] The smart card reader 280 reads the smart card, in step 405, and extracts the identity therefrom. Then, in step 410, the smart card reader 280 forwards the identity to the printer's CPU 200. The CPU 200 receives the identity in step 415 and generates a message including the identity, in step 420, which it forwards to the document store 130 in step 425.

[0056] In step 430, the document store 130 receives the message and, in step 435, searches the hard disk 135 for any documents having the same identity. In the present embodiment, the document store 130 will find one document. However, in general, there may be none, or any number of documents having a matching identity stored on the hard disk 135. At this stage, the document store 130 and printer 140 may be arranged to interact to provide status information to the recipient, displayed on a front panel display 270 of the printer, for example showing the number of documents awaiting printing, or that there are no documents waiting.

[0057] Next, in step 440, the document store 130 returns to the printer 140 only the envelope for the document having the matching identity. In principle, the document could be sent at this stage as well, although whether or not this is done depends on the size of the document and the amount of available printer buffer memory. It is believed preferable at present to retrieve only the envelope, unless the printer 140 has a significant amount of RAM 240 into which the whole document could be received.

[0058] In step 445, the printer receives the envelope and, in step 450, forwards the encrypted session key to the smart card reader 280. The smart card reader 280 transfers the encrypted session key to the smart card, and the smart card, in turn, decrypts the session key, in step 455, using the private key stored therein. The smart card outputs the decrypted session key, in step 460, and the smart card reader 280 forwards the session key to the CPU 200, in step 465.

[0059] This technique for retrieving the session key is extremely advantageous, since the private key never needs to leave the smart card, and thus remains secret.

[0060] The printer 140 forwards a message to the document store 130, in step 470, for the document store to transmit the encrypted document to the printer 140. In step 475, the document store 130 receives the message and, in step 480, transmits the document to the printer 140. In step 485, the printer 140 receives the document and, in step 490, deciphers it back into page description language using the session key.

[0061] Finally, in step 495, the printer prints the document for the intended recipient.

[0062] It will be appreciated that the network 110 could be a local area network, a wide area network or even global area network. For example, for the case of a global area network, the local computer 100 could be situated in an office in London and the printer could be located in an airport in Tokyo or New York. Similarly, the directory server 120 and the document store 130 could be located anywhere in the world.

[0063] In some embodiments, for responsiveness purposes, it may be desirable to have mirror document stores (not shown) - similar to Internet mirror sites - where the data in one store is copied by the store to other, geographically distant document stores. Thus, for example, there may be a London-based data server, and Tokyo and New York-based data servers. On receiving a document, the London data server would copy the document to both the Tokyo and New York data servers so that the recipient could retrieve and print the document from the data server nearest the printer being used. Obviously, the data mirroring could be tuned if it is known where the recipient is most likely to be when he wishes to print the document. For example, if the recipient were likely to be in New York, but might instead be in London, then a document submitted in London would only be mirrored to the New York-based data server. Such recipient location information could form part of the user profile information stored by the directory server 120. Thus, the location information under these circumstances would also be returned to the local computer 100 with the public key information, and this information would also be forwarded to the document store 130.

[0064] It is envisaged that the directory server 120 will hold other user profile information. For example, a recipient may only ever wish to receive documents from one specified printer. In this case, the information returned by the directory server 120 would reflect this and the document store 130 would then only release the encrypted document to the specified printer. Other information held by the directory server 120 for particular users might include printer information, which determines how the document is formatted by the local computer 100, for example whether to format the document into PostScript or PCL. In general, it is expected that the user can access the directory server 120, for example via the Internet, and modify his user profile whenever required.

[0065] It will also be appreciated that the components and processes described above need not reside on different computers. For example, the local computer 100 could support the directory server and document store processes, as well as a secure printer process.

[0066] Furthermore, there is no reason why any or all of the processes described herein could not be located and called from any of a number of different computer systems connected to the distributed environment. Having said this, it is important, although not essential, that documents that require secure printing do not pass across any publicly accessible or low security communications channels, without being in an encrypted state.

Claims

1. Hardcopy apparatus arranged for receiving, decrypting and rendering documents, the hardcopy apparatus comprising:

   interface means for receiving from a document source an encrypted document;
   processing means configured for decrypting the encrypted document; and
   rendering means for producing a hard copy of the decrypted document.

2. Hardcopy apparatus according to claim 1, further comprising input/output means for communicating with a removable processing means.

3. Hardcopy apparatus according to claim 3, wherein the input/output means is a smart card reader and the removable processing means is a smart card received by the smart card reader.

4. Hardcopy apparatus according to claim 4, wherein the processing means is configured for receiving information from the smart card reader, when a smart card is received thereby, and using the information to retrieve and decrypt an encrypted document.

5. Hardcopy apparatus according claim 4, wherein the processing means is configured for:

   receiving from the smart card an identity and sending a first message via the interface means to the document source, the message including at least an indication of the identity; and
   receiving from the document source via the interface means, in response to the first message, a return message including at least an encrypted session key for an encrypted document stored by the document source and having a matching identity.

6. Hardcopy apparatus according to claim 5, wherein the processing means is configured for sending the encrypted session key to the smart card reader, for the smart card to extract the session key, and receiving back the session key.

7. Hardcopy apparatus according to claim 6, wherein the processing means is configured for using the session key to decrypt the encrypted document.

8. Hardcopy apparatus according to any one of the preceding claims, comprising a printer.

9. Hardcopy apparatus according to any one of claims 1 to 7, comprising a facsimile machine.

10. A method of controlling hardcopy apparatus to render an encrypted document, comprising the steps of:

    retrieving from a document source an encrypted document;
    decrypting the encrypted document; and
    rendering the document to produce a hardcopy thereof.

11. A method according to claim 10, further comprising the step of providing the hardcopy apparatus with identity information, to determine which document the hardcopy apparatus retrieves.

12. A method according to claim 10 or claim 11, further comprising the step of providing the hardcopy apparatus with decryption information to enable the hardcopy apparatus to decrypt the retrieved document.

13. A method according to claim 11 or claim 12, wherein the identity information is stored on a smart card and is transferred to the hardcopy apparatus by means of a smart card reader associated with the hardcopy apparatus.

14. A method according to any one of claims 10 to 13, further comprising the step of retrieving from the document source an envelope associated with the encrypted document, the envelope comprising a session key encrypted using a public key encryption algorithm, decrypting the session key using a corresponding private key, and decrypting the document using the session key.

15. A method according to claim 13, wherein the step of decrypting the session key is enacted by a smart card, which is received by a smart card reader associated with the hardcopy apparatus.

16. A computer system arranged for secure rendering of documents, the system comprising:

    secure printing means for encrypting a document for an intended recipient and forwarding to a document store means the encrypted document with identity information of the intended

recipient;

document store means for receiving encrypted documents and respective identity information and storing said encrypted documents and respective information, and for receiving requests from hardcopy apparatus for documents having a specific identity and sending respective documents to the respective requesting hardcopy apparatus; and

hardcopy apparatus arranged for requesting of the document store means transfer of encrypted documents having a specific identity, decrypting received documents and rendering in hardcopy form decrypted documents.

17. A computer system as claimed in claim 16, wherein the secure printing means is arranged for enacting public key encryption and the hardcopy apparatus is arranged for providing corresponding private key decryption.

18. A computer system as claimed in claim 16 or claim 17, wherein the hardcopy apparatus is arranged for sending data that is encrypted with a public key to a removable processing means for decryption thereby using a corresponding private key.

19. A computer system as claimed in claim 18, wherein the hardcopy apparatus comprises a smart card reader and the removable processing source is a smart card.

20. A document server, comprising document processing means arranged for:

receiving encrypted documents;
storing encrypted documents;
receiving requests for specific documents;
searching the stored documents for the specific documents; and
returning found documents to the requesting party.

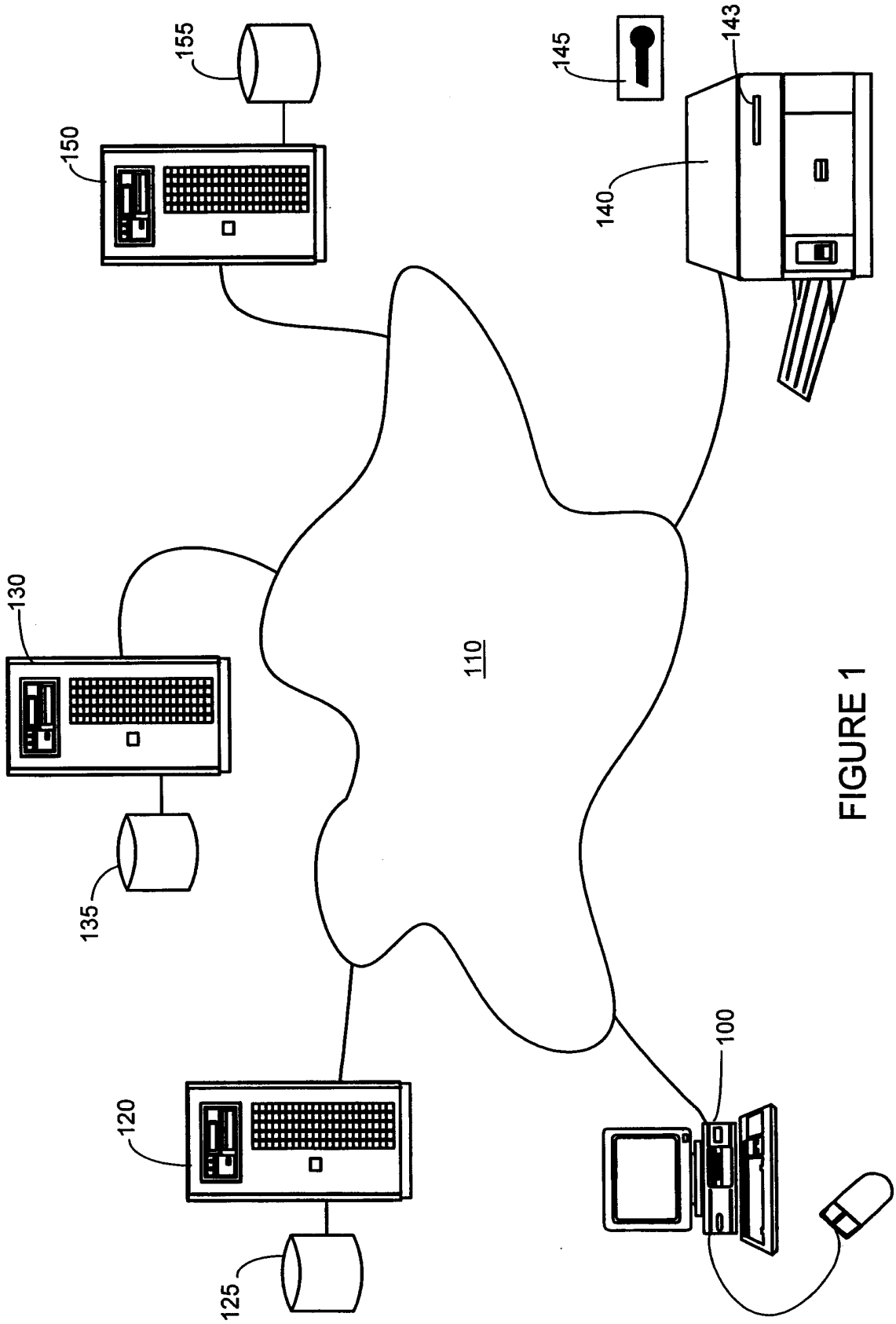

FIGURE 1

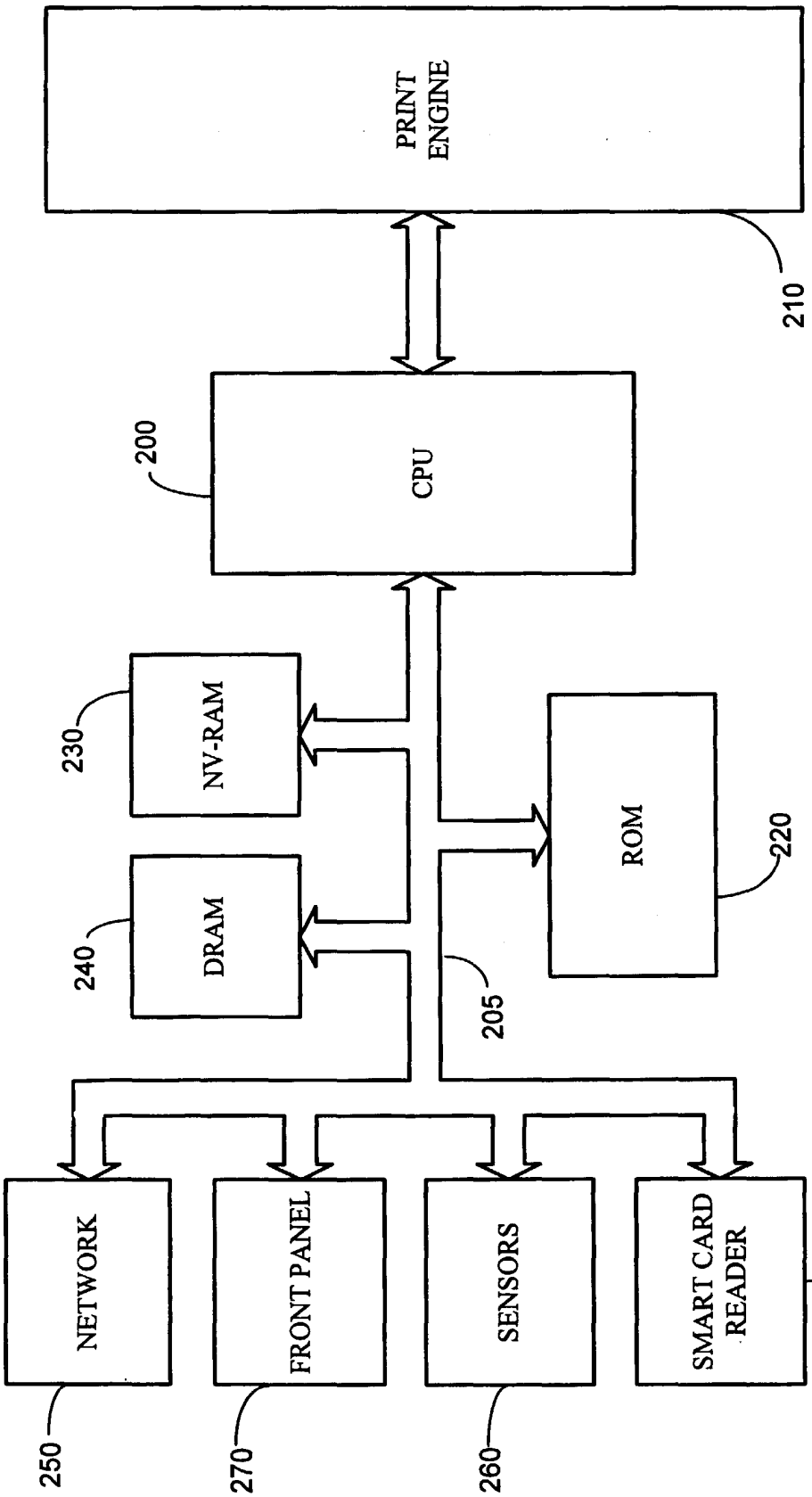
PRINT ENGINE
210
CPU
200
NV-RAM
230
DRAM
240
ROM
220
205
NETWORK
250
FRONT PANEL
270
SENSORS
260
SMART CARD READER
280

FIGURE 2

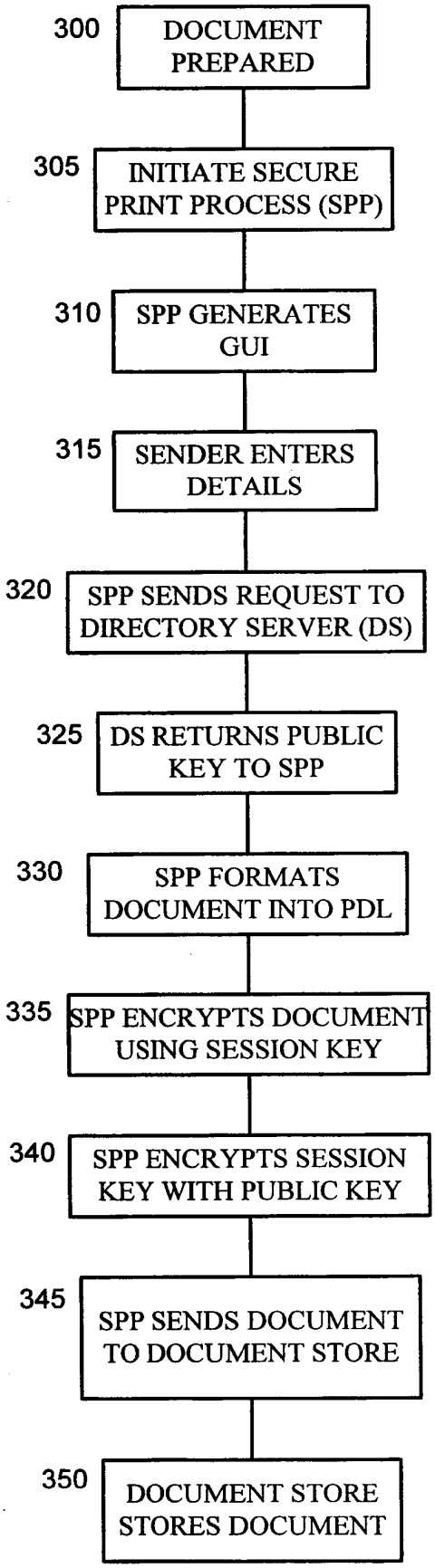
300
DOCUMENT PREPARED
305
INITIATE SECURE PRINT PROCESS (SPP)
310
SPP GENERATES GUI
315
SENDER ENTERS DETAILS
320
SPP SENDS REQUEST TO DIRECTORY SERVER (DS)
325
DS RETURNS PUBLIC KEY TO SPP
330
SPP FORMATS DOCUMENT INTO PDL
335
SPP ENCRYPTS DOCUMENT USING SESSION KEY
340
SPP ENCRYPTS SESSION KEY WITH PUBLIC KEY
345
SPP SENDS DOCUMENT TO DOCUMENT STORE
350
DOCUMENT STORE STORES DOCUMENT

FIGURE 3.

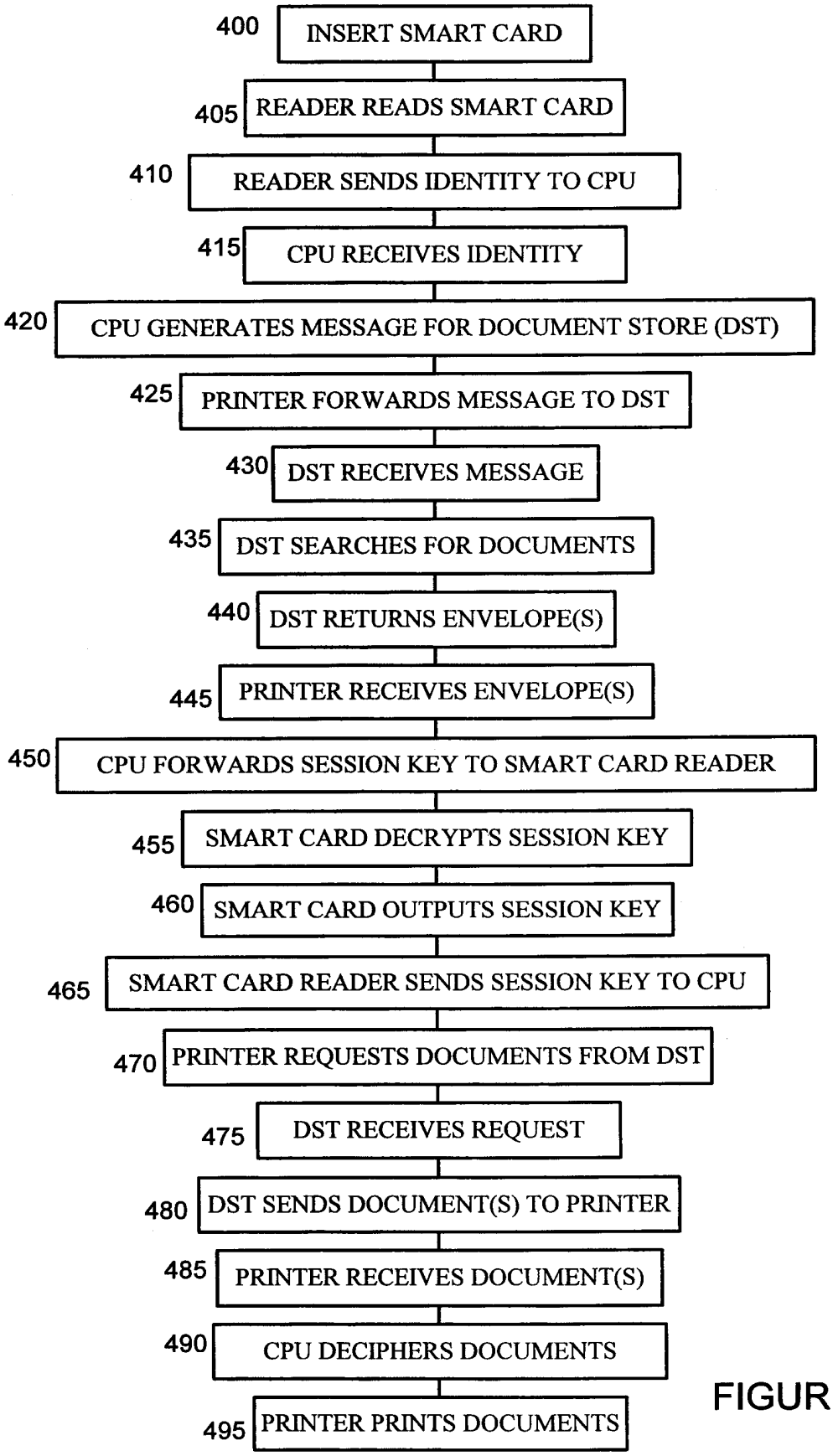
400
INSERT SMART CARD
405
READER READS SMART CARD
410
READER SENDS IDENTITY TO CPU
415
CPU RECEIVES IDENTITY
420
CPU GENERATES MESSAGE FOR DOCUMENT STORE (DST)
425
PRINTER FORWARDS MESSAGE TO DST
430
DST RECEIVES MESSAGE
435
DST SEARCHES FOR DOCUMENTS
440
DST RETURNS ENVELOPE(S)
445
PRINTER RECEIVES ENVELOPE(S)
450
CPU FORWARDS SESSION KEY TO SMART CARD READER
455
SMART CARD DECRYPTS SESSION KEY
460
SMART CARD OUTPUTS SESSION KEY
465
SMART CARD READER SENDS SESSION KEY TO CPU
470
PRINTER REQUESTS DOCUMENTS FROM DST
475
DST RECEIVES REQUEST
480
DST SENDS DOCUMENT(S) TO PRINTER
485
PRINTER RECEIVES DOCUMENT(S)
490
CPU DECIPHERS DOCUMENTS
495
PRINTER PRINTS DOCUMENTS

FIGURE 4

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 30 0144

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP 0 665 486 A (AT & T CORP) 2 August 1995 * figure 2 * * column 1, line 34 - column 2, line 5 * * column 4, line 50 - column 5, line 40 * ---	1-5,8, 10-12, 14,16, 17,20	G06F1/00
A	GB 2 267 986 A (ALGORITHMIC RES LTD) 22 December 1993 * figures 1,11,13 * * page 4, line 5 - line 31 * * page 5, line 28 - page 7, line 25 * * page 10, line 25 - line 35 * -----	1-6,8, 10-19	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

G06F
H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	19 June 1998	WEISS, P

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 30 0144

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-06-1998

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0665486 A	02-08-1995	US 5509074 A	16-04-1996
		CA 2137065 A	28-07-1995
		JP 7239828 A	12-09-1995
GB 2267986 A	22-12-1993	IL 103062 A	04-08-1996
		EP 0587375 A	16-03-1994
		SG 43927 A	14-11-1997
		US 5406624 A	11-04-1995

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82